IN THE CLAIMS:

1. (Currently Amended) A security gateway for securely connecting a plurality of networks; comprising:

a logical interface to a first network;

a logical interface to a second network;

a physical interface to a third network that is an untrusted network;

a logical interface to a fourth network, via said third network, that is a protected resource network;

a processor configured to execute packet handling rules for:

denying at least some client access through the gateway from a host in the untrusted network to hosts in the first network, in the second network and in the protected resource network;

denying at least some client access through the gateway from a host in the second network to a host in the first network; and

permitting at least some client access through the gateway from a host in the first network to hosts in the second network and in the protected resource network.

2. (Original) The security gateway of claim 1, wherein the processor is further configured to execute packet handling rules for translating a source network address in a packet sent to the second network.

3. (Original) The security gateway of claim 2, wherein the packet handling rules for translating translate the source network address of a packet sent to the second network to be the network address of the security gateway interface to the second network.

4. (Original) The security gateway of claim 1, wherein the processor is further configured to execute packet handling rules for permitting at least some client access through the gateway from a host in the first network to a host in the untrusted network.

5. (Original) The security gateway of claim 4, wherein the processor is further configured to execute packet handling rules for translating a source network address in a packet sent to the untrusted network.

6. (Original) The security gateway of claim 5, wherein the packet handling rules for translating translate the source network address of a packet sent to the untrusted network to be the network address of the security gateway interface to the untrusted network.

7. (Original) The security gateway of claim 1, wherein the processor is further configured to execute packet handling rules for permitting at least some client access through the gateway from a host in the protected resource network to a host in the first network.

8. (Original) The security gateway of claim 1, wherein the processor is further configured to execute packet handling rules for denying at least some client access through the gateway from a host in the protected resource network to a host in the first network.

9. (Original) The security gateway of claim 1, wherein the processor is further configured to execute packet handling rules for permitting at least some client access through the gateway from a host in the second network to a host in the untrusted network.

10. (Original) The security gateway of claim 9, wherein the processor is further configured to execute packet handling rules for translating a source network address in a packet sent to the untrusted network.

11. (Original) The security gateway of claim 10, wherein the packet handling rules for translating translate the source network address of a packet sent to the untrusted network to be the network address of the security gateway interface to the untrusted network.

12. (Original) The security gateway of claim 1, further comprising a protected network service, and the processor is further configured to execute packet handling rules

for denying at least some access from at least one network to the protected network service.

13. (Original) The security gateway of claim 12, wherein the protected network service is a mail relay.

14. (Original) The security gateway of claim 1, wherein the interface to the protected resource network includes a VPN tunnel utilizing the untrusted network.

15. (Original) The security gateway of claim 1, wherein the processor is further configured to execute packet handling rules for denying at least some client access through the gateway from a host in the protected resource network to a host in the second network.

16. (Original) The security gateway of claim 1, wherein the processor is further configured to execute packet handling rules for denying at least some client access through the gateway from a host in the protected resource network to a host in the untrusted network.

17. (Original) The security gateway of claim 1, wherein the processor is further configured to execute packet handling rules for denying at least some client access through the gateway from a host in the second network to a host in the protected resource network.

18. (Original) The security gateway of claim 1, wherein the logical interface to the first network is a logical interface to a first trust-group network, and the logical interface to the second network is a logical interface to a second trust-group network.

19. (Original) The security gateway of claim 1, wherein the logical interface to the first network is a logical interface to a first local network, and the logical interface to the second network is a logical interface to a second local network.

20. (Original) The security gateway of claim 1, wherein the logical interface to the protected resource network is a logical interface to a remote corporate network.

21. (Original) The security gateway of claim 1, wherein the processor is further configured to execute packet handling rules for:

denying at least some client access through the gateway from a host in the second network to a host in the protected resource network; and

denying at least some client access through the gateway from a host in the protected resource network to hosts in the second network and in the untrusted network.

22. (Original) The security gateway of claim 21, wherein the interface to the protected resource network includes a VPN tunnel utilizing the untrusted network.

23. (Original) The security gateway of claim 22, wherein the processor is further configured to execute packet handling rules for permitting at least some client access through the gateway from a host in the second network to a host in the untrusted network.

24. (Original) The security gateway of claim 23, wherein the processor is further configured to execute packet handling rules for permitting at least some client access through the gateway from a host in the first network to a host in the untrusted network.

25. (Currently Amended) A machine readable medium containing configuration instructions for performing a method for securely connecting a plurality of networks through a security gateway having a logical interface to a first network, a logical interface to a second network, a physical interface to a third network that is an untrusted network and a logical interface to a fourth network that is a protected resource network where said logical interface to said fourth network is via said third network, the method comprising the steps of:

denying at least some client access through the gateway from a host in the untrusted network to hosts in the first network, in the second network and in the protected resource network;

denying at least some client access through the gateway from a host in the second network to a host in the first network; and

permitting at least some client access through the gateway from a host in the first network to hosts in the second network and in the protected resource network.

26. (Original) The machine readable medium of claim 25, wherein the method further comprises the step of translating a source network address in a packet sent to the second local network.

27. (Original) The machine readable medium of claim 26, wherein the translating step includes translating the source network address of a packet sent to the second network to be the network address of the security gateway interface to the second network.

28. (Original) The machine readable medium of claim 25, wherein the method further comprises the step of permitting at least some client access through the gateway from a host in the first network to a host in the untrusted network.

29. (Original) The machine readable medium of claim 28, wherein the method further comprises the step of translating a source network address in a packet sent to the untrusted network.

30. (Original) The machine readable medium of claim 29, wherein the translating step includes translating the source network address of a packets sent to the untrusted network to be the network address of the security gateway interface to the untrusted network.

31. (Original) The machine readable medium of claim 25, wherein the method further comprises the step of permitting at least some client access through the gateway from a host in the protected resource network to a host in the first network.

32. (Original) The machine readable medium of claim 25, wherein the method further comprises the step of denying at least some client access through the gateway from a host in the protected resource network to a host in the first network.

33. (Original) The machine readable medium of claim 25, wherein the method further comprises the step of permitting at least some client access through the gateway from a host in the second network to a host in the untrusted network.

34. (Original) The machine readable medium of claim 33, wherein the method further comprises the step of translating a source network address in a packet sent to the untrusted network.

35. (Original) The machine readable medium of claim 34, wherein the translating step includes translating the source network address of a packet sent to the untrusted network to be the network address of the security gateway interface to the untrusted network.

36. (Original) The machine readable medium of claim 25, wherein the security gateway further has a protected network service, and the method further comprises the step of denying at least some access from at least one network to the protected network service.

37. (Original) The machine readable medium of claim 36, wherein the protected network service is a mail relay.

38. (Original) The machine readable medium of claim 25, wherein the interface to the protected resource network includes a VPN tunnel utilizing the untrusted network.

39. (Original) The machine readable medium of claim 25, wherein the method further comprises the step of denying at least some client access through the gateway from a host in the protected resource network to a host in the second network.

40. (Original) The machine readable medium of claim 25, wherein the method further comprises the step of denying at least some client access through the gateway from a host in the protected resource network to a host in the untrusted network.

41. (Original) The machine readable medium of claim 25, wherein the method further comprises the step of denying at least some client access through the gateway from a host in the second network to a host in the protected resource network.

42. (Currently Amended) A method for securely connecting a plurality of networks through a security gateway having a logical interface to a first network, a logical interface to a second network, a physical interface to a third network that is an untrusted network and a logical interface to a fourth network that is a protected resource network, said logical interface to said fourth network being via said third network; the method comprising the steps of:

denying at least some client access through the gateway from a host in the untrusted network to hosts in the first network, in the second network and in the protected resource network;

denying client access from a host in the second network to a host in the first network; and

permitting client access from a host in the first network to hosts in the second network and in the protected resource network.

43. (Original) The method of claim 42, further comprising the step of translating a source network address in a packet sent to the second network.

44. (Original) The method of claim 43, wherein the translating step includes translating the source network address of a packet sent to the second network to be the network address of the security gateway interface to the second network.

45. (Original) The method of claim 42, further comprising the step of permitting at least some client access through the gateway from a host in the first network to a host in the untrusted network.

46. (Original) The method of claim 45, further comprising the step of translating a source network address in a packet sent to the untrusted network.

47. (Original) The method of claim 46, wherein the translating step includes translating the source network address of a packet sent to the untrusted network to be the network address of the security gateway interface to the untrusted network.

48. (Original) The method of claim 42, further comprising the step of permitting at least some client access through the gateway from a host in the protected resource network to a host in the first network.

49. (Original) The method of claim 42, further comprising the step of denying at least some client access through the gateway from a host in the protected resource network to a host in the first network.

50. (Original) The method of claim 42, further comprising the step of permitting at least some client access through the gateway from a host in the second network to a host in the untrusted network.

51. (Original) The method of claim 50, further comprising the step of translating a source network address in a packet sent to the untrusted network.

52. (Original) The method of claim 51, wherein the translating step includes translating the source network address of a packet sent to the untrusted network to be the network address of the security gateway interface to the untrusted network.

53. (Original) The method of claim 52, wherein the security gateway further has a protected network service, and the method further comprises the step of denying at least some access from at least one network to the protected network service.

54. (Original) The method of claim 53, wherein the protected network service is a mail relay.

55. (Original) The method of claim 42, wherein the interface to the protected resource network includes a VPN tunnel utilizing the untrusted network.

56. (Original) The method of claim 42, further comprising the step of denying at least some client access through the gateway from a host in the protected resource network to a host in the second network.

57. (Original) The method of claim 42, further comprising the step of denying at least some client access through the gateway from a host in the protected resource network to a host in the untrusted network.

58. (Original) The method of claim 42, further comprising the step of denying at least some client access through the gateway from a host in the second network to a host in the protected resource network.